

10/13

John -

Based on our visit  
last week to FBI head-  
quarters, we're going to  
take another look at  
including FBI programs  
in this effort.

Al

# INFORMATION

ROUTING AND RECORD SHEET				
SUBJECT: (Optional)				
FROM: Charles A. Briggs Executive Director		EXTENSION	NO. <b>ER 83-3704</b>	
			DATE	
TO: (Officer designation, room number, and building)	DATE		OFFICER'S INITIALS	COMMENTS (Number each comment to show from whom to whom. Draw a line across column after each comment.)
	RECEIVED	FORWARDED		
1. <i>DM</i> DDCI	25 JUL 1983		<i>DM</i>	STAT
2.				
3. <div style="border: 1px solid black; width: 150px; height: 20px; display: inline-block;"></div> <i>000 / ICS</i>				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				

DCI/ICS 83-4042  
18 October 1983

MEMORANDUM FOR: Deputy Director of Central Intelligence

VIA: Director, Intelligence Community Staff  
Deputy Director, Intelligence Community Staff

FROM: Ruth M. Davis, COMPUSEC Project Director

SUBJECT: Minimum Security SAFEGUARDS for  
"Critical Systems"

REFERENCES: A. DDCI Memo to D/ICS dtd 6 May 1983, Subject:  
Minimum Computer Security Standards  
B. Dr. Ruth Davis' Memo to DDCI dtd 13 Oct 1983,  
Subject: Selection of "Critical Systems"  
C. D/ICS Memo to DDCI dtd 6 June 1983,  
Subject: Minimum Computer Security Standards

1. Action Requested: That you review the attached draft set of Minimum SAFEGUARDS for Protection of "Critical Systems" Processing Intelligence Information, and that you approve my proceeding with a field evaluation of the proposed SAFEGUARDS at the selected critical system sites before imposing them as mandatory. ☐

25X1

2. Background: As a result of Reference A and as agreed upon at the COMPUSEC Executive Steering Group meeting of 27 June 1983, it was requested that members submit candidate critical systems for which a set of "minimum" SAFEGUARDS would be developed under the auspices of a COMPUSEC Working Group. Based on the DDCI's direction at the 27 June 1983 meeting, the critical systems for which these SAFEGUARDS would be mandated are identified in Reference B. ☐ IC Staff, was asked to chair a SAFEGUARDS working group made up of members of the Executive Steering Group agencies. This group completed its formulation of a draft report specifying 41 SAFEGUARDS on 3 October. ☐

25X1

25X1

3. The 41 proposed SAFEGUARDS represent stringent security controls for the 13 selected critical systems. They make full use of the DOD Computer Security Evaluation Center's criteria as suggested in the DDCI's memorandum of 6 May 1983, Reference A. ☐

25X1

4. Based on Reference C, these "minimum" SAFEGUARDS are intended to serve as a short-term answer to the lack of minimum standards for the selected 13 critical systems. They do not substitute for the longer term development of a Computer Security Standards Policy and a standards enforcement mechanism. ☐

25X1

25X1

~~SECRET~~

SECRET

5. Discussion: Significant disagreements exist within various elements of DOD over the utility of the DOD Computer Security Evaluation Center's criteria, upon which many of the SAFEGUARDS in the attached proposal are based. A critical aspect of this debate centers on enforceability; a topic being addressed separately from the SAFEGUARDS Working Group. It is now imperative to involve the critical systems' management to: determine the impact SAFEGUARD implementation would have on operations; assess implementation costs; and establish some measure of their enforceability. Your authorization is necessary for this approach. It will take about eight weeks to complete the field evaluation and requires deferring your decision on promulgation of the attached package until the results are completed and available for your consideration. The results are not likely to cause you to make any major change in the proposed "minimum" SAFEGUARDS but it will provide a firm basis for making them mandatory. ☐

25X1

6. Recommendation: That you review the attached package to determine if the SAFEGUARDS meet your approval, but that you defer a decision to impose them as mandatory until the completion of field evaluation. That you specifically authorize a COMPUSEC SAFEGUARDS Evaluation Group under Mr. ☐ leadership to proceed immediately with field coordination for the 13 critical systems. ☐

25X1

25X1



Ruth M. Davis

Attachment: a/s

APPROVED:

---

Deputy Director of Central Intelligence

---

Date

DISAPPROVED:

---

Deputy Director of Central Intelligence

---

Date

SECRET

SUBJECT: Minimum Security SAFEGUARDS for  
"Critical Systems"

DISTRIBUTION:

Orig - Adse

1 - Executive Registry

1 - D/ICS

1 - D/PPS

1 - ICS Registry

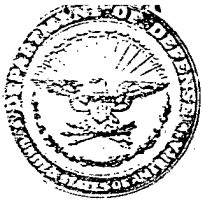
1 - IHC Subject (LGS)

1 - IHC Chrono

ICS/IHC

(18 Oct 83)

25X1



DEFENSE INTELLIGENCE AGENCY

WASHINGTON, D.C. 20301

Executive Registry

83-3637

CONFIDENTIAL

15 JUL 1983

C-14,095/RSE-4

MEMORANDUM FOR THE DEPUTY DIRECTOR OF CENTRAL INTELLIGENCE

SUBJECT: Candidate Critical Systems (U)

1. (C) Reference is made to your memorandum of 8 July 1983 concerning the identification of DoD's "critical systems" for the purpose of review by Dr. Davis' Computer Security Group. DIA has defined "critical systems" as those DoD systems which provide essential intelligence to the National Command Authorities, the Joint Chiefs of Staff, the Military Services, the Unified and Specified Commands, the U.S. Intelligence Community and intelligence information releaseable to NATO and Allied military forces. The attachment contains our list of candidate systems.

2. (C) I continue to support Dr. Davis' efforts; however, I want to ensure we have a fully developed, controlled and mutually agreed upon approach before we begin to subject these systems to intense security review. In this regard, it is necessary to apply some conditions on the use of the enclosed list. The listed "critical systems" have been accredited by the Director, DIA or the Senior Intelligence Officer of the DoD component that is Executive Agent for the system. These systems meet or exceed the minimum security requirements of DCID 1/16, DIA Manual 50-4 and/or DoD Directive 5030.58, as applicable. Accordingly, I desire to be consulted (and my personal approval given) before Dr. Davis or anyone from her study group contacts or visits the organizations that are responsible for these systems. Further, I trust that any recommendations for security changes or enhancements to these systems will be presented for my consideration, as DoD's Senior Intelligence Officer, before implementation.

1 Enclosure  
List of Candidate Critical  
Systems (C), 1 cy

JAMES A. WILLIAMS  
Lieutenant General, U. S. Army  
Director

CLASSIFIED BY: DIA/RSE-4  
DECLASSIFY ON: OADR

CONFIDENTIAL

## C O N F I D E N T I A L

## CANDIDATE CRITICAL SYSTEMS

SYSTEM NAME (ACRONYM)	EXECUTIVE AGENT
Communications Support Processor (CSP)	• AIR FORCE ✓
Interim Tactical ELINT Processor (ITEP)	• ARMY ✓
Ground Mobile Command Capability (GMCC)	• ARMY ✓
Ocean Surveillance Information System (OSIS)	• NAVY ✓
Modular Architecture for the Exchange of Information (MAXI)	• AIR FORCE ✓
Defense Intelligence Agency On Line System (DIAOLS)	• DIA ✓
Automated Imagery Reporting and Exploitation System (AIRES)	• DIA ✓
Defense Dissemination System (DDS)	• DIA ✓
Central Information Reference and Control (CIRC)	• AIR FORCE ✓
Support for the Analyst File Environment (SAFE D)	• DIA ✓
Tactical Reconnaissance Exploitation Demonstration System (TREDS)	• AIR FORCE
Korean Air Intelligence System (KAIS)	• AIR FORCE ✓
Satellite Reconnaissance Advanced Notice Program (SATRAN)	• ADCOM
SWL (contractor)	• NAVY

C O N F I D E N T I A L

Washington, D.C. 20505

8 JUL 1983

MEMORANDUM FOR: Executive Steering Group for the Dr. Davis  
Computer Security Project

SUBJECT: Summary of First Steering Group Meeting

1. Your comments and suggestions at our first meeting on 27 June 1983 regarding the proposed tasks identified by Ruth Davis and her project team are most appreciated. The tasks that we have agreed to are complex, but there is a sense of urgency about getting on with this project.

25X1

2. We have changed the name of the project back to the Computer Security (COMPSEC) project to reflect the major element of the effort. The scope of the project includes more than just computer security, as reflected in paragraph 3 below. The COMPSEC project should not be confused with or perceived as being in competition with the various computer security efforts ongoing within the Intelligence Community [(e.g., the DoD Computer Security Evaluation Center (CSEC))].

3. Ruth will incorporate your recommendations into her revised project plans. Based on the comments provided at the meeting, the scope of the effort (Issue 1) will be bounded as follows:

- o Exclude stand-alone word processors (initially)
- o Exclude single-user systems such as remote sensing equipment
- o Include computer systems and telecommunications systems utilizing computers that serve multiple users
- o Initially include those automated systems processing sensitive compartmented intelligence (SCI) and automated systems processing collateral intelligence information that could compromise sensitive methods and sources (e.g., clandestine HUMINT reports from CIA/DDO or SIGINT sensitive reports)

DC25X1  
EXEC  
REG

SECRET

- o Exclude US Government systems processing collateral intelligence other than that noted in the preceding bullet ☐

25X1

4. Our near-term goal is to identify known or suspected vulnerabilities, assess the risk to sensitive operating systems, establish a sense of criticality for developing and applying procedural and hardware safeguards, and by doing so assure ourselves that the methods and sources as well as the intelligence itself are properly protected while supporting all vital operations. ☐

25X1

5. In regard to issue 5, the proposed redefinition of minimum standards to "safeguards for reducing critical vulnerabilities" is accepted and the task statement will be adjusted accordingly. ☐

25X1

6. The task of identifying "critical systems" will require your personal attention due to the sensitivity of the topic within the National Security arena and the implications to our positive intelligence activities. Please provide to me by 13 July 1983 a candidate list of systems for our joint review and discussion. After our review those few systems identified and designated as critical will be assigned to the appropriate COMPSEC working group. ☐

25X1

7. We may need more than the time planned to complete several of the proposed efforts, but we should push forward. Ruth will let us know how much more time she may need when we review the next progress report in July. ☐

25X1

8. Your active participation and personal support in this important effort is appreciated. ☐

25X1

/s/ John N. McMahon

John N. McMahon

2  
SECRET

DCI/ICS 83-4444  
6 July 1983

MEMORANDUM FOR: Deputy Director of Central Intelligence

VIA: Director, Intelligence Community Staff  
Deputy Director, Intelligence Community Staff

*Carly* JUL 1983

FROM: [redacted] Executive Secretary  
Computer Security Steering Group

25X1

SUBJECT: Summary of First Steering Group Meeting

1. Attached for your signature is a proposed memorandum to the steering group members summarizing the activities of our first meeting. Dr. Davis and I feel that it is appropriate to respond to the comments made by the members and to proceed with the effort as soon as possible.

2. The identification of "critical systems" is understood by the members to be a most sensitive issue and will take some hand holding. Clearly the producers of intelligence should be the first to come forward and once the users are convinced you mean business they will also participate. You should expect this task to take a couple of cycles before everyone is forthcoming and committed.

3. The issue of how to prepare a threat briefing that will be convincing without jeopardizing current operations will be looked after by Evan Hineman, [redacted] and MG Burt Stubblebine.

25X1

4. Request your signature on the attachment.

25X1

Attachment:  
a/s



SECRET